

ABSTRACT:

A method, system, and medium for assessing and/or managing risks for an organization is described. The method, for example, comprises the steps of inventorying a number of assets of the organization, identifying at least one criterion defining a security objective 5 of the organization, and identifying one or more inventoried assets that relate to the identified criterion. The assets may include one or more computers, networking equipment therefor and physical locations where the computers and networking equipment are located. The method may also include the step of formulating one or more metric equations, each metric equation being defined, in part, by the one or more 10 identified assets. Each metric equation yields an outcome value when one or more measurements are made relating to the identified assets. The method may also include the step of assessing the risk to the organization based on the measured values of the one or more metric equations. Corresponding system, medium and means are also described.